State of Indiana Policy and Standards

Secure File Transfer and File Storage

Standard ID
IOT-CS-ARC-003

Published Date
10/3/2016

Effective Date
10/3/2016

Last Updated
9/28/2016

Next Review Date
9/28/2017

Policy
01.0 Asset Management (ID.AM)

01.3 ID.AM-3

01.3.1 System Connections

Purpose
Securely store and move confidential and non-confidential files throughout all zones and tiers.

Scope
IOT Supported Entities

Statement
The following security controls shall be followed with any solution transferring and storing files within the State of Indiana or with non-state personnel.

Boundary Protection

- Confidential files shall only reside in the Protected Zone (PZ)
- Unencrypted confidential files shall not reside on any Server Message Block (SMB) file share in any zone
- Must utilize an IOT managed reverse proxy technology to prevent direct access to files between untrusted zones
- Must integrate with IOT's Data Loss Prevention (DLP) and Anti-virus/Malware solution
    - Files outbound from the Protected Zone (PZ) shall be scanned with DLP for confidential data and flagged accordingly
    - Files inbound to any zone must be scanned with Anti-virus
    - Files residing in the Protected must be scanned on regular intervals
- The prevention of commingling of an agency's transitory files with another agency's files will be centrally managed with IOT's Manage File Transfer solution
- Transitory files will have a minimal lifespan when residing on the IOT Managed File Transfer solution

Least Privilege

- Must use your privilege account while accessing files from confidential servers
- Utilize IOT's Active Directory and/or Lightweight Directory Access Protocol (LDAP) for role based authentication

Encryption

- All files in-transit and at rest shall follow IOT Data Encryption standard

Logging

- Real-time monitoring of inbound and outbound transfers
- Provide and send both audit and application logs to enterprise SIEM

Other

- Support Application to Application (A2A) and Ad Hoc/manual transfers
- Only provide file transfer-related features and functionality
- Support workflow and automation of file transfer-related activities and processes

Roles

Information Asset Owners/System Owners

Responsibilities

Information Asset Owners/System Owners shall ensure that all files being stored and transferred are utilizing an IOT compliant file storage and managed file transfer solution

Management Commitment

Management shall ensure that their staff are educated and required to use the Secure File Transfer and File Storage standard

Coordination Among Organizational Entities

Agencies can reference the technical File Transfer and File Storage Standards or contact the Enterprise Architecture and Hosting Services Groups for compliant file storage and managed file transfer solutions

Compliance

Agencies shall review all related standards to fully understand the requirements around transferring and storing files. New agency employees must review these standards as part of their on-boarding process.

Exceptions

Exceptions will be handled on a case by case basis through the Director of Risk & Compliance, State CISO and the IOT Architect team